REMARKS

Favorable reconsideration of this application is respectfully requested in view of the foregoing amendments and the following remarks.

No claims have been canceled or added by this response. Claims 1, 3, 5, 8, 13, 15, 16, 18, 22-25, 27, 28 and 34 have been amended. Thus, claims 1, 3-5, 8, 13, 15-18, 22-25, 27, 28, 34, 35, 41 and 43 are pending in the present application, of which claims 1, 3, 5, 8, 13, 15, 16, 18, 22-25, 27, 28, 34 and 35 are independent.

Claims 1, 3-5, 8, 13, 15-18, 22-24, 34, 41 and 43 are rejected under 35 U.S.C. §103(a) as being unpatentable over Spiegel et al. (US Patent No. 7,159,149, hereinafter Spiegel) in view of Willebeek-LeMair et al. (US Publication No. 20030204632, hereinafter Willebeek-LeMair).

Claims 25, 27, 28 and 35 are rejected under 35 U.S.C. §103(a) as being unpatentable over Spiegel in view of Willebeek-LeMair and further in view of Bunker et al. (US Publication No. 20030056116, hereinafter Bunker). Applicants amended the claims and traverse the rejections for the following reasons.

As an example, amended independent claims 1 and 13 each recite (among other things) the following features:

> changing the measurement parameters when the communication is judged to have been executed by the worm at the judging,
>
> wherein the acquiring includes acquiring, based on the measurement parameters changed at the changing, the information on the communication judged to have been executed by the worm at the judging.

As will be explained below, at least the above features of amended claims 1 and 13 are a distinction over Spiegel, and thus over its combination with Willebeek-LeMair.

Spiegel discloses at column 5, lines 15-21, column 5, lines 47-53 and column 6, lines 15-26, "... This technique allows for the threshold criteria to be dynamic, adapting to the particular operating environment of each system...", "... the failed attempts are weighted according to an attribute thereof, such as the source 10,20 of the failed attempt or the destination address." and "... an embodiment of the WDS 100 ...", respectively.

However, Spiegel fails to disclose or suggest:

> changing the measurement parameters when the communication is judged to have been executed by the worm at the judging,
>
> wherein the acquiring includes acquiring, based on the measurement parameters changed at the changing, the information on the communication judged to have been executed by the worm at the judging. (Underlining added for emphasis).

Willebeek-LeMair discloses the following at paragraph [0056]

> the agent 126 operates to assess changes to the network 14 detected by the network discovery functionality 112, confirm their validity, and inform the intrusion detector functionality 116 to tune its operation so that false alerts are not generated when the new, but nonetheless valid, information types are encountered in the network traffic content.

In the above disclosure, tuning "its operation" is performed for "when the new, but nonetheless valid, information types are encountered in the network traffic content", but not for "the communication judged to have been executed by the worm at the judging" as recited in amended claims amended 1 and 13.

Hence, Willebeek-LeMair also fails to disclose or suggest:

> changing the measurement parameters when the communication is judged to have been executed by the worm at the judging,
>
> wherein the acquiring includes acquiring, based on the measurement parameters changed at the changing, the information on the communication judged to have been executed by the worm at the judging.

Hence, the noted features of amended claims 1 and 13, namely the following, are a distinction over Spiegel and also Willebeek-LeMair either alone or in combination.

> changing the measurement parameters when the communication is judged to have been executed by the worm at the judging,
>
> wherein the acquiring includes acquiring, based on the measurement parameters changed at the changing, the information on the communication judged to have been executed by the worm at the judging.

Among other things, a *prima facie* case of obviousness must establish that the asserted combination of references teaches or suggests each and every element of the claimed invention. In view of the distinction of amended claims 1 and 13 noted above, at least one claimed element is not present in the asserted combination of references. Hence, the Office Action fails to establish a *prima facie* case of obviousness vis-à-vis amended claims 1 and 13. Claim 4 depends from claim 1, and so at least similarly distinguishes over the asserted combination of references.

As an example, amended independent claim 15 recites (among other things) the following features:

> a setting changing unit that changes the measurement parameters when the communication is judged to have been executed by the worm by the judging unit, wherein
>
> the acquiring unit acquires, based on the measurement parameters changed by the setting changing unit, the information on the communication judged to have been executed by the worm by the judging unit.

As will be explained below, at least the features of amended claim 15 are a distinction over Spiegel, and thus over its combination with Willebeek-LeMair.

Spiegel discloses at column 5, lines 15-21, column 5, lines 47-53 and column 6, lines 15-26, "... This technique allows for the threshold criteria to be dynamic, adapting to the particular operating environment of each system...", "... the failed attempts are weighted according to an attribute thereof, such as the source 10,20 of the failed attempt or the destination address..." and "... an embodiment of the WDS 100 ...", respectively.

However, Spiegel fails to disclose or suggest:

> a setting changing unit that changes the measurement parameters when the communication is judged to have been executed by the worm by the judging unit, wherein
>
> the acquiring unit acquires, based on the measurement parameters changed by the setting changing unit, the information on the communication judged to have been executed by the worm by the judging unit. (Underlining added for emphasis).

Willebeek-LeMair discloses the following at paragraph [0056].

> the agent 126 operates to assess changes to the network 14 detected by the network discovery functionality 112, confirm their validity, and inform the intrusion detector functionality 116 to tune its operation so that false alerts are not generated when the new, but nonetheless valid, information types are encountered in the network traffic content.

In the above disclosure, tuning "its operation" is performed for "when the new, but nonetheless valid, information types are encountered in the network traffic content", but not for "the communication judged to have been executed by the worm by the judging unit", as recited in amended claim 15.

Hence, Willebeek-LeMair also fails to disclose or suggest:

> a setting changing unit that changes the measurement parameters when the communication is judged to have been executed by the worm by the judging unit, wherein
>
> the acquiring unit acquires, based on the measurement parameters changed by the setting changing unit, the information on the communication judged to have been executed by the worm by the judging unit.

Hence, the noted features of amended claim 15, namely the following, are a distinction over Spiegel and also Willebeek-LeMair, either alone or in combination.

> a setting changing unit that changes the measurement parameters when the communication is judged to have been executed by the worm by the judging unit, wherein
>
> the acquiring unit acquires, based on the measurement parameters changed by the setting changing unit, the information on the communication judged to have been executed by the worm by the judging unit.

Among other things, a *prima facie* case of obviousness must establish that the asserted combination of references teaches or suggests each and every element of the claimed invention. In view of the distinction of amended claim 15 noted above, at least one claimed element is not present in the asserted combination of references. Hence, the Office Action fails to establish a *prima facie* case of obviousness vis-à-vis claim 15. Claim 17 depends from claim 15, and so at least similarly distinguishes over the asserted combination of references.

As an example, amended independent claim 3 recites (among other things) the following features:

> changing the judgment criteria when the communication is judged to have been executed by the worm at the judging, wherein
> the judging includes further judging whether the communication judged to have been executed by the worm at the judging has been executed by the worm based on the information acquired and the judgment criteria changed at the changing.

As will be explained below, at least the features of claim 3 are a distinction over Spiegel, and thus over its combination with Willebeek-LeMair.

Spiegel discloses at column 5, lines 8-10, column 5, lines 15-21, column 5, lines 47-53 and column 6, lines 15-22, "... the threshold criteria are based on historical data for failed connection attempts and the diversity thereof that are obtained over time...", "... This technique allows for the threshold criteria to be dynamic, adapting to the particular operating environment of each system", "... the failed attempts are weighted according to an attribute thereof, such as the source 10,20 of the failed attempt or the destination address..." and "... an embodiment of the WDS 100 ...", respectively.

However, Spiegel fails to disclose or suggest:

> changing the judgment criteria when the communication is judged to have been executed by the worm at the judging, wherein
> <u>the judging includes further judging whether the communication judged to have been executed by the worm at the judging has been executed by the worm</u> based on the information

> acquired and the judgment criteria changed at the changing. (Underlining added for emphasis).

Willebeek-LeMair discloses the following at paragraph [0056].

> the agent 126 operates to assess changes to the network 14 detected by the network discovery functionality 112, confirm their validity, and inform the intrusion detector functionality 116 to tune its operation so that false alerts are not generated when the new, but nonetheless valid, information types are encountered in the network traffic content.

In the above disclosure, tuning "its operation" is performed for "when the new, but nonetheless valid, information types are encountered in the network traffic content". Hence, Willebeek-LeMair also fails to disclose or suggest:

> changing the judgment criteria when the communication is judged to have been executed by the worm at the judging, wherein
>
> the judging includes further judging whether the communication judged to have been executed by the worm at the judging has been executed by the worm based on the information acquired and the judgment criteria changed at the changing. (Underlining added for emphasis).

Hence, the noted features of amended claim 3, namely the following, are a distinction over Spiegel and also Willebeek-LeMair, either alone or in combination.

> changing the judgment criteria when the communication is judged to have been executed by the worm at the judging, wherein
>
> the judging includes further judging whether the communication judged to have been executed by the worm at the judging has been executed by the worm based on the information acquired and the judgment criteria changed at the changing.

Among other things, a *prima facie* case of obviousness must establish that the asserted combination of references teaches or suggests each and every element of the claimed invention. In view of the distinction of amended claim 3 noted above, at least one claimed element is not present in the asserted combination of references. Hence, the Office Action fails to establish a *prima facie* case of obviousness vis-à-vis claim 3. Claim 41 depends from claim 3, and so at least similarly distinguishes over the asserted combination of references.

As an example, amended independent claim 16 recites (among other things) the following features:

> a setting changing unit that changes the judgment criteria when the communication is judged to have been executed by the worm by the judging unit, wherein
>
> the judging unit further judges whether the communication judged to have been executed by the worm by the judging unit has been executed by the worm based on the information acquired by the acquiring unit and the judgment criteria changed by the setting changing unit.

As will be explained below, at least the features of amended claim 16 are a distinction over Spiegel, and thus over its combination with Willebeek-LeMair.

Spiegel discloses at column 5, lines 8-10, column 5, lines 15-21, column 5, lines 47-53 and column 6, lines 15-22, "... the threshold criteria are based on historical data for failed connection attempts and the diversity thereof that are obtained over time...", "... This technique allows for the threshold criteria to be dynamic, adapting to the particular operating environment of each system", "... the failed attempts are weighted according to an attribute thereof, such as the source 10,20 of the failed attempt or the destination address..." and "... an embodiment of the WDS 100 ...", respectively.

However, Spiegel fails to disclose or suggest:

> a setting changing unit that changes the judgment criteria when the communication is judged to have been executed by the worm by the judging unit, wherein
>
> <u>the judging unit further judges whether the communication judged to have been executed by the worm by the judging unit has been executed by the worm</u> based on the information acquired by the acquiring unit and the judgment criteria changed by the setting changing unit. (Underlining added for emphasis).

Willebeek-LeMair discloses the following at paragraph [0056].

> the agent 126 operates to assess changes to the network 14 detected by the network discovery functionality 112, confirm their validity, and inform the intrusion detector functionality 116 to tune its operation so that false alerts are not generated when the new, but nonetheless valid, information types are encountered in the network traffic content.

In the above disclosure, tuning "its operation" is performed for "when the new, but nonetheless valid, information types are encountered in the network traffic content". Hence, Willebeek-LeMair also fails to disclose or suggest:

> a setting changing unit that changes the judgment criteria when the communication is judged to have been executed by the worm by the judging unit, wherein
>
> the judging unit further judges whether the communication judged to have being executed by the worm by the judging unit has been executed by the worm based on the information acquired by the acquiring unit and the judgment criteria changed by the setting changing unit. (Underlining added for emphasis).

Hence, the noted features of claim 16, namely the following, are a distinction over Spiegel and also Willebeek-LeMair, either alone or in combination.

> a setting changing unit that changes the judgment criteria when the communication is judged to have been executed by the worm by the judging unit, wherein
>
> the judging unit further judges whether the communication judged to have been executed by the worm by the judging unit has been executed by the worm based on the information acquired by the acquiring unit and the judgment criteria changed by the setting changing unit.

Among other things, a *prima facie* case of obviousness must establish that the asserted combination of references teaches or suggests each and every element of the claimed invention. In view of the distinction of amended claim 16 noted above, at least one claimed element is not present in the asserted combination of references. Hence, the Office Action fails to establish a *prima facie* case of obviousness vis-à-vis amended claim 16.

As an example, amended independent claim 5 recites (among other things) the following features:

> the second judging includes judging that a plurality of computers in the predetermined network segment are infected by the worm when all three conditions are satisfied, the three conditions being that
>
> a communication from the computer in the predetermined network segment is judged to be infected by the worm at the first judging,
>
> a number of communication packets that are transmitted from the predetermined network segment to the outside becomes greater than a number of the communication packets transmitted from the predetermined network segment to the outside when the computer is judged to be infected by the worm at the first judging, and
>
> a number of destination addresses of the communication packets that are transmitted from the predetermined network segment to the outside becomes greater than a number of destination addresses of the communication packets transmitted from the predetermined network segment to the outside when the computer Is judged to be infected by the worm at the first judging.

As will be explained below, at least the features of amended claim 5 are a distinction over Spiegel, and thus over its combination with Willebeek-LeMair.

Spiegel discloses at column 5, lines 8-10, column 5, lines 47-50, column 6, lines 15-22 and column 3, lines 20-27, "... the threshold criteria are based on historical data for failed connection attempts and the diversity thereof that are obtained over time...", "... the failed attempts are weighted according to an attribute thereof, such as the source 10,20 of the failed attempt or the destination address.", "... an embodiment of the WDS 100 ..." and "... If infected, a process 20 is likely to produce a relatively large number of connection attempts to remote destination addresses over a given period of time...", respectively.

Spiegel also discloses at column 1, lines 50-60, column 1, lines 60-67, column 3, line 63 to column 4, line 9, "... a network monitoring module (110) observes (205) failed network connection attempts from multiple sources (10,20)...", "... this determination is based on a set of threshold criteria..." and the following, respectively.

> ... the threshold criteria include any one or a combination of the following metrics: (1) the number of failed network connection attempts; (2) the diversity of destination network addresses associated with the failed network connection attempts; (3) the randomness of the failed addresses; and (4) a weighting for each failed network connection attempt according to an attribute thereof (e.g., source or destination address).

However, Spiegel fails to disclose or suggest the following:

> the second judging includes judging that a plurality of computers in the predetermined network segment are infected by the worm <u>when all three conditions are satisfied</u>, the three conditions being that
>
> a communication from the computer in the predetermined network segment is judged to be infected by the worm at the first judging,
>
> a number of communication packets that are transmitted from the predetermined network segment to the outside becomes greater than a number of the communication packets transmitted from the predetermined network segment to the outside when the computer is judged to be infected by the worm at the first judging, and
>
> a number of destination addresses of the communication packets that are transmitted from the predetermined network segment to the outside becomes greater than a number of destination addresses of the communication packets transmitted from the predetermined network segment to the outside when the computer is judged to be infected by the worm at the first judging. (Underlining added for emphasis).

Hence, the noted features of claim 5, namely the following, are a distinction over Spiegel.

> the second judging includes judging that a plurality of computers in the predetermined network segment are infected by the worm when all three conditions are satisfied, the three conditions being that

> a communication from the computer in the predetermined network segment is judged to be infected by the worm at the first judging,
>
> a number of communication packets that are transmitted from the predetermined network segment to the outside becomes greater than a number of the communication packets transmitted from the predetermined network segment to the outside when the computer is judged to be infected by the worm at the first judging, and
>
> a number of destination addresses of the communication packets that are transmitted from the predetermined network segment to the outside becomes greater than a number of destination addresses of the communication packets transmitted from the predetermined network segment to the outside when the computer is judged to be infected by the worm at the first judging.

The noted features also are a distinction over Willebeek-LeMair as evidenced, e.g., by the Office Action. That is, the Office Action does not assert Willebeek-LeMair as disclosing the noted features.

Among other things, a *prima facie* case of obviousness must establish that the asserted combination of references teaches or suggests each and every element of the claimed invention. In view of the distinction of amended claim 5 noted above, at least one claimed element is not present in the asserted combination of references. Hence, the Office Action fails to establish a *prima facie* case of obviousness vis-à-vis amended claim 5.

As an example, amended independent claim 18 recites (among other things) the following features:

> the judging unit judges at the second time that a plurality of computers in the predetermined network segment are infected by the worm when all three conditions are satisfied, the three conditions being that
>
> a communication from the computer in the predetermined network segment is judged at the first time to be infected by the worm,
>
> a number of communication packets that are transmitted from the predetermined network segment to the outside becomes greater than a number of the communication packets transmitted from the predetermined network segment to the outside when the

> computer is judged at the first time to be infected by the worm, and
>
> a number of destination addresses of the communication packets that are transmitted from the predetermined network segment to the outside becomes greater than a number of destination addresses of the communication packets transmitted from the predetermined network segment to the outside when the computer is judged at the first time to be infected by the worm.

As will be explained below, at least the features of amended claim 18 are a distinction over Spiegel, and thus over its combination with Willebeek-LeMair.

Spiegel discloses at column 5, lines 8-10, column 5, lines 47-50, column 6, lines 15-22 and column 3, lines 20-27, "... the threshold criteria are based on historical data for failed connection attempts and the diversity thereof that are obtained over time...", "... the failed attempts are weighted according to an attribute thereof, such as the source 10,20 of the failed attempt or the destination address.", "... an embodiment of the WDS 100 ..." and "... If infected, a process 20 is likely to produce a relatively large number of connection attempts to remote destination addresses over a given period of time...", respectively.

Spiegel also discloses at column 1, lines 50-60, column 1, lines 60-67, column 3, line 63 to column 4, line 9, "... a network monitoring module (110) observes (205) failed network connection attempts from multiple sources (10,20)...", "... this determination is based on a set of threshold criteria..." and the following, respectively.

> ... the threshold criteria include any one or a combination of the following metrics: (1) the number of failed network connection attempts; (2) the diversity of destination network addresses associated with the failed network connection attempts; (3) the randomness of the failed addresses; and (4) a weighting for each failed network connection attempt according to an attribute thereof (e.g., source or destination address).

However, Spiegel fails to disclose or suggest the following:

> the judging unit judges at the second time that a plurality of computers in the predetermined network segment are infected by

> the worm when all three conditions are satisfied, the three conditions being that
>
> a communication from the computer in the predetermined network segment is judged at the first time to be infected by the worm,
>
> a number of communication packets that are transmitted from the predetermined network segment to the outside becomes greater than a number of the communication packets transmitted from the predetermined network segment to the outside when the computer is judged at the first time to be infected by the worm, and
>
> a number of destination addresses of the communication packets that are transmitted from the predetermined network segment to the outside becomes greater than a number of destination addresses of the communication packets transmitted from the predetermined network segment to the outside when the computer is judged at the first time to be infected by the worm. (Underlining added for emphasis).

Hence, the noted features of amended claim 18, namely the following, are a distinction over Spiegel.

> the judging unit judges at the second time that a plurality of computers in the predetermined network segment are infected by the worm when all three conditions are satisfied, the three conditions being that
>
> a communication from the computer in the predetermined network segment is judged at the first time to be infected by the worm,
>
> a number of communication packets that are transmitted from the predetermined network segment to the outside becomes greater than a number of the communication packets transmitted from the predetermined network segment to the outside when the computer is judged at the first time to be infected by the worm, and
>
> a number of destination addresses of the communication packets that are transmitted from the predetermined network segment to the outside becomes greater than a number of destination addresses of the communication packets transmitted from the predetermined network segment to the outside when the computer is judged at the first time to be infected by the worm.

The noted features also are a distinction over Willebeek-LeMair as evidenced, e.g., by the Office Action. That is, the Office Action does not assert Willebeek-LeMair as disclosing the noted features.

Among other things, a *prima facie* case of obviousness must establish that the asserted combination of references teaches or suggests each and every element of the claimed invention. In view of the distinction of amended claim 18 noted above, at least one claimed element is not present in the asserted combination of references. Hence, the Office Action fails to establish a *prima facie* case of obviousness vis-à-vis amended claim 18.

As an example, amended independent claim 8 recites (among other things) the following feature:

> the judging includes identifying a type of the worm by comparing features of a first communication with features of a second communication executed by a worm that are recorded in advance, when the first communication is judged to be executed by a worm.

As will be explained below, at least the feature of amended claim 8 is a distinction over Spiegel, and thus over its combination with Willebeek-LeMair.

Spiegel discloses at column 3, lines 58-67, column 6, lines 15-22 and column 5, lines 8-15, "... the heuristic is implemented with a set of threshold criteria that embodies whether the failed connection attempts associated with a source are non-normal...", "... an embodiment of the WDS 100 ..." and the following, respectively.

> ... the threshold criteria are based on historical data for failed connection attempts and the diversity thereof that are obtained over time. These collected data are taken and defined as typical failure rates for normal operating conditions...

However, Spiegel fails to disclose or suggest the following:

> the judging includes identifying a type of the worm by comparing features of a first communication with features of a second communication executed by a worm that are recorded in advance, <u>when the first communication is judged to be executed by a worm</u>. (<u>Underlining</u> added for emphasis).

In the above, the "comparing features of a first communication" is performed not for judging whether the first communication is executed by a worm, but for "identifying a type of the worm".

Hence, the noted feature of claim 8, namely the following, is a distinction over Spiegel.

> the judging includes identifying a type of the worm by comparing features of a first communication with features of a second communication executed by a worm that are recorded in advance, when the first communication is judged to be executed by a worm.

The noted feature also is a distinction over Willebeek-LeMair as evidenced, e.g., by the Office Action. That is, the Office Action does not assert Willebeek-LeMair as disclosing the noted feature.

Among other things, a *prima facie* case of obviousness must establish that the asserted combination of references teaches or suggests each and every element of the claimed invention. In view of the distinction of amended claim 8 noted above, at least one claimed element is not present in the asserted combination of references. Hence, the Office Action fails to establish a *prima facie* case of obviousness vis-à-vis amended claim 8. Claim 43 depends from claim 8, and so at least similarly distinguishes over the asserted combination of references.

As an example, amended independent claims 22 and 23 each recite (among other things) the following feature:

> the extracting includes summing up a number of the communication packets for each port number, the communication packets being transmitted in the communication when the communication is judged to have been executed by the worm at the judging, and extracting as the reference information, a most frequently appeared port number of the communication packets transmitted in the communication judged to have been executed by the worm at the judging.

As will be explained below, at least the feature of claims 22 and 23 is a distinction over Willebeek-LeMair, and thus over its combination with Spiegel.

Willebeek-LeMair discloses the following at paragraph [0031], lines 5-14.

> the extraction of packet features may comprise features 38(1) from the header portion 34 (such as, for example, destination and source IP address, destination and source ports, and the like).

However, Willebeek-LeMair fails to disclose or suggest the following:

> the extracting includes summing up a number of the communication packets for each port number, the communication packets being transmitted in the communication when the communication is judged to have been executed by the worm at the judging, and extracting as the reference information, a most frequently appeared port number of the communication packets transmitted in the communication judged to have been executed by the worm at the judging. (Underlining added for emphasis).

The above underlined recitation indicates that "summing up" and "extracting" are performed for the packets transmitted in "the communication judged to have been executed by the worm".

Hence, the noted feature of amended claims 22 and 23, namely the following, is a distinction over Willebeek-LeMair.

> the extracting includes summing up a number of the communication packets for each port number, the communication packets being transmitted in the communication when the communication is judged to have been executed by the worm at the judging, and extracting as the reference information, a most frequently appeared port number of the communication packets transmitted in the communication judged to have been executed by the worm at the judging.

The noted feature also is a distinction over Spiegel as evidenced, e.g., by the Office Action. That is, the Office Action does not assert Spiegel as disclosing the noted feature.

Among other things, a *prima facie* case of obviousness must establish that the asserted combination of references teaches or suggests each and every element of the claimed invention. In view of the distinction of amended claims 22 and 23 noted above, at least one claimed element is not present in the asserted combination of references. Hence, the Office Action fails to establish a *prima facie* case of obviousness vis-à-vis amended claims 22 and 23.

As an example, amended independent claim 24 recites (among other things) the following feature:

> the reference information extracting unit sums up a number of the communication packets for each port number, the communication packets being transmitted in the communication when the communication is judged to have been executed by the worm by the judging unit, and extracts, as the reference information, a most frequently appeared port number of the communication packets transmitted in the communication judged to have been executed by the worm by the judging unit.

As will be explained below, at least the feature of claim 24 is a distinction over Willebeek-LeMair, and thus over its combination with Spiegel.

Willebeek-LeMair discloses the following at paragraph [0031], lines 5-14.

> the extraction of packet features may comprise features 38(1) from the header portion 34 (such as, for example, destination and source IP address, destination and source ports, and the like)

However, Willebeek-LeMair fails to disclose or suggest the following:

> the reference information extracting unit <u>sums up</u> a number of the communication packets for each port number, the communication packets being transmitted in the communication <u>when the communication is judged to have been executed by the worm by the judging unit</u>, and <u>extracts</u>, as the reference information, a most frequently appeared port number of the communication packets transmitted in <u>the communication judged to have been executed by the worm by the judging unit</u>. (<u>Underlining</u> added for emphasis).

The above underlined recitation indicates that "sums up" and "extracts" are performed for the packets transmitted in "the communication judged to have been executed by the worm".

Hence, the noted feature of claim 24, namely the following, is a distinction over Willebeek-LeMair.

> the reference information extracting unit sums up a number of the communication packets for each port number, the communication packets being transmitted in the communication when the communication is judged to have been executed by the worm by the judging unit, and extracts, as the reference information, a most frequently appeared port number of the communication packets transmitted in the communication judged to have been executed by the worm by the judging unit.

The noted feature also is a distinction over Spiegel as evidenced, e.g., by the Office Action. That is, the Office Action does not assert Spiegel as disclosing the noted feature.

Among other things, a *prima facie* case of obviousness must establish that the asserted combination of references teaches or suggests each and every element of the claimed invention. In view of the distinction of amended claim 24 noted above, at least one claimed element is not present in the asserted combination of references. Hence, the Office Action fails to establish a *prima facie* case of obviousness vis-à-vis amended claim 24.

As an example, amended independent claim 34 recites (among other things) the following feature:

> the reference information extracting unit sums up a number of the communication packets for each port number, the communication packets being transmitted in the communication when the communication is judged to have been executed by the worm by the worm judging unit, and extracts, as the reference information, a most frequently appearing port number of the communication packets transmitted in the communication judged to have been executed by the worm by the worm judging unit.

As will be explained below, at least the feature of amended claim 34 is a distinction over Willebeek-LeMair, and thus over its combination with Spiegel.

Willebeek-LeMair discloses the following at paragraph [0031], lines 5-14.

> the extraction of packet features may comprise features 38(1) from the header portion 34 (such as, for example, destination and source IP address, destination and source ports, and the like).

However, Willebeek-LeMair fails to disclose or suggest the following:

> the reference information extracting unit sums up a number of the communication packets for each port number, the communication packets being transmitted in the communication when the communication is judged to have been executed by the worm by the worm judging unit, and extracts, as the reference information, a most frequently appearing port number of the communication packets transmitted in the communication judged to have been executed by the worm by the worm judging unit. (Underlining added for emphasis).

The above underlined recitation indicates that "sums up" and "extracts" are performed for the packets transmitted in "the communication judged to have been executed by the worm".

Hence, the noted feature of claim 34, namely the following, is a distinction over Willebeek-LeMair.

> the reference information extracting unit sums up a number of the communication packets for each port number, the communication packets being transmitted in the communication when the communication is judged to have been executed by the worm by the worm judging unit, and extracts, as the reference information, a most frequently appearing port number of the communication packets transmitted in the communication judged to have been executed by the worm by the worm judging unit.

The noted feature also is a distinction over Spiegel as evidenced, e.g., by the Office Action. That is, the Office Action does not assert Spiegel as disclosing the noted feature.

Among other things, a *prima facie* case of obviousness must establish that the asserted combination of references teaches or suggests each and every element of the claimed invention. In view of the distinction of amended claim 34 noted above, at least one claimed element is not present in the asserted combination of references. Hence, the Office Action fails to establish a *prima facie* case of obviousness vis-à-vis amended claim 34.

As an example, amended independent claims 25 and 27 each recite (among other things) the following feature:

> the extracting further includes summing up, for each direction of communication of a packet transmitted out from the predetermined network segment or transmitted to the predetermined network segment, a number of the communication packets transmitted in the communication upon it being judged that the communication is executed by the worm at the judging, and extracting, as the reference information, a direction of the communication wherein the number of the communication packets is over a threshold value.

(Please note that the Office Action refers to a wrong recitation as shown below, which is not recited in claims 25 and 27.)

> extracting further includes summing up, for each type of the communication, a number of the communication packets transmitted in the communication upon it being judged that the communication is executed by the worm at the judging, and extracting, as the reference information, a—type of the communication, the number of the communication packets is over a threshold value.

As will be explained below, at least the feature of claims 25 and 27 is a distinction over Bunker, and thus over its combination with Spiegel and Willebeek-LeMair.

Bunker discloses at paragraph [0189], lines 1-11, paragraph [0215], lines 1-5 and paragraph [0220], lines 8-12, "The format of an Enterprise-Wide Summary report includes number of hosts tested; number of new hosts appearing on network; ..." and the following, respectively.

> Vulnerability Trending shows total counts of vulnerabilities as well as counts grouped by risk level. Summary graphical information depicts severity, likely impact, skill level needed to exploit, and likely cause of vulnerabilities

> ... The Standard Report shows vulnerability trending showing total counts of vulnerabilities as well as counts grouped by risk level; fix reports showing count of vulnerabilities corrected vs. those left unresolved as well as a risk level of fixed and unfixed vulnerabilities; ...

However, Bunker fails to disclose or suggest the following:

> the extracting further includes summing up, for each direction of communication of a packet transmitted out from the predetermined network segment or transmitted to the predetermined network segment, a number of the communication packets transmitted in the communication upon it being judged that the communication is executed by the worm at the judging, and extracting, as the reference information, a direction of the communication wherein the number of the communication packets is over a threshold value. (Underlining added for emphasis)

Hence, the noted feature of claims 25 and 27, namely the following, is a distinction over Bunker.

> the extracting further includes summing up, for each direction of communication of a packet transmitted out from the predetermined network segment or transmitted to the predetermined network segment, a number of the communication packets transmitted in the communication upon it being judged that the communication is executed by the worm at the judging, and extracting, as the reference information, a direction of the communication wherein the number of the communication packets is over a threshold value.

The noted feature also is a distinction over Spiegel and Willebeek-LeMair as evidenced, e.g., by the Office Action. That is, the Office Action does not assert Spiegel and Willebeek-LeMair as disclosing the noted feature.

Among other things, a *prima facie* case of obviousness must establish that the asserted combination of references teaches or suggests each and every element of the claimed invention. In view of the distinction of amended claims 25 and 27 noted above, at least one claimed element is not present in the asserted combination of references. Hence, the Office Action fails to establish a *prima facie* case of obviousness vis-à-vis amended claims 25 and 27.

As an example, independent claim 28 recites (among other things) the following feature:

> the reference information extracting unit further sums up, for each direction of communication of a packet transmitted out from the predetermined network segment or transmitted to the predetermined network segment, a number of the communication packets transmitted in the communication upon it being judged that the communication is executed by the worm by the judging unit, and extracts, as the reference information, a direction of the communication wherein the number of the communication packets is over a threshold value.

(Please note that the Office Action refers to a wrong recitation as shown below, which is not recited in claim 28.)

> extracting further includes summing up, for each type of the communication, a number of the communication packets transmitted in the communication upon it being judged that the communication is executed by the worm at the judging, and extracting, as the reference information, a—type of the communication, the number of the communication packets is over a threshold value.

As will be explained below, at least the feature of claim 28 is a distinction over Bunker, and thus over its combination with Spiegel and Willebeek-LeMair.

Bunker discloses at paragraph [0189], lines 1-11, paragraph [0215], lines 1-5 and paragraph [0220], lines 8-12, "The format of an Enterprise-Wide Summary report includes number of hosts tested; number of new hosts appearing on network; ..." and the following, respectively.

> Vulnerability Trending shows total counts of vulnerabilities as well as counts grouped by risk level. Summary graphical information depicts severity, likely impact, skill level needed to exploit, and likely cause of vulnerabilities

> ... The Standard Report shows vulnerability trending showing total counts of vulnerabilities as well as counts grouped by risk level; fix reports showing count of vulnerabilities corrected vs. those left unresolved as well as a risk level of fixed and unfixed vulnerabilities; ...

However, Bunker fails to disclose or suggest the following:

> the reference information extracting unit further <u>sums up, for each direction of communication of a packet transmitted out from the predetermined network segment or transmitted to the predetermined network segment, a number of the communication packets transmitted in the communication upon it being judged that the communication is executed by the worm by the judging unit</u>, and extracts, as the reference information, a direction of the communication wherein the number of the communication packets is over a threshold value. (Underlining added for emphasis).

Hence, the noted feature of claim 28, namely the following, is a distinction over Bunker.

> the reference information extracting unit further sums up, for each direction of communication of a packet transmitted out from the predetermined network segment or transmitted to the predetermined network segment, a number of the communication packets transmitted in the communication upon it being judged that the communication is executed by the worm by the judging unit, and extracts, as the reference information, a direction of the communication wherein the number of the communication packets is over a threshold value.

The noted feature also is a distinction over Spiegel and Willebeek-LeMair as evidenced, e.g., by the Office Action. That is, the Office Action does not assert Spiegel and Willebeek-LeMair as disclosing the noted feature.

Among other things, a *prima facie* case of obviousness must establish that the asserted combination of references teaches or suggests each and every element of the claimed invention. In view of the distinction of amended claim 28 noted above, at least one claimed element is not present in the asserted combination of references. Hence, the Office Action fails to establish a *prima facie* case of obviousness vis-à-vis amended claim 28.

As an example, independent claim 35 recites (among other things) the following feature:

> the reference information extracting unit further sums up, for each direction of communication of a packet transmitted out from the predetermined network segment or transmitted to the predetermined network segment, a number of the communication packets transmitted in the communication upon it being judged by the worm judging unit that the communication is executed by the worm, and extracts, as the reference information, a direction of the communication wherein the number of the communication packets is over a threshold value.

(Please note that the Office Action refers to a wrong recitation as shown below, which is not recited in claim 35.)

> extracting further includes summing up, for each type of the communication, a number of the communication packets transmitted in the communication upon it being judged that the communication is executed by the worm at the judging, and extracting, as the reference information, a—type of the communication, the number of the communication packets is over a threshold value.

As will be explained below, at least the feature of claim 35 is a distinction over Bunker, and thus over its combination with Spiegel and Willebeek-LeMair.

Bunker discloses at paragraph [0189], lines 1-11, paragraph [0215], lines 1-5 and paragraph [0220], lines 8-12, "The format of an Enterprise-Wide Summary report includes number of hosts tested; number of new hosts appearing on network; ..." and the following, respectively.

> Vulnerability Trending shows total counts of vulnerabilities as well as counts grouped by risk level. Summary graphical information depicts severity, likely impact, skill level needed to exploit, and likely cause of vulnerabilities

> ... The Standard Report shows vulnerability trending showing total counts of vulnerabilities as well as counts grouped by risk level; fix reports showing count of vulnerabilities corrected vs. those left unresolved as well as a risk level of fixed and unfixed vulnerabilities; ...

However, Bunker fails to disclose or suggest the following:

> the reference information extracting unit further sums up, for each direction of communication of a packet transmitted out from the predetermined network segment or transmitted to the predetermined network segment, a number of the communication packets transmitted in the communication upon it being judged by the worm judging unit that the communication is executed by the worm, and extracts, as the reference information, a direction of the communication wherein the number of the communication packets is over a threshold value. (Underlining added for emphasis).

Hence, the noted feature of claim 35, namely the following, is a distinction over Bunker.

> the reference information extracting unit further sums up, for each direction of communication of a packet transmitted out from the predetermined network segment or transmitted to the predetermined network segment, a number of the communication packets transmitted in the communication upon it being judged by the worm judging unit that the communication is executed by the worm, and extracts, as the reference information, a direction of the communication wherein the number of the communication packets is over a threshold value.

The noted feature also is a distinction over Spiegel and Willebeek-LeMair as evidenced, e.g., by the Office Action. That is, the Office Action does not assert Spiegel and Willebeek-LeMair as disclosing the noted feature.

Among other things, a *prima facie* case of obviousness must establish that the asserted combination of references teaches or suggests each and every element of the claimed invention. In view of the distinction of claim 35 noted above, at least one claimed element is not present in the asserted combination of references.

Hence, the Office Action fails to establish a *prima facie* case of obviousness vis-à-vis claim 35.

In view of the foregoing discussion, the rejection of claims 1, 3-5, 8, 13, 15-18, 22-25, 27, 28, 34, 35, 41 and 43 is traversed. Accordingly, withdrawal of the §103(a) rejection is respectfully requested.

For all of the foregoing reasons, Applicants submit that this Application is in condition for allowance, which is respectfully requested. The Examiner is invited to contact the undersigned attorney if an interview would expedite prosecution.

If a Petition under 37 C.F.R. §1.136(a) for an extension of time for response is required to make the attached response timely, it is hereby petitioned under 37 C.F.R. §1.136(a) for an extension of time for response in the above-identified application for the period required to make the attached response timely. The Commissioner is hereby authorized to charge any additional fees which may be required to this Application under 37 C.F.R. §§1.16-1.17, or credit any overpayment, to Deposit Account No. 07-2069.

Respectfully submitted,

By Joseph P. Fox
Joseph P. Fox
Registration No. 41,760

Customer No. 24978
November 11, 2009
300 South Wacker Drive
Suite 2500
Chicago, Illinois 60606
Telephone: (312) 360-0080
Facsimile: (312) 360-9315